CERTIFICATE POLICY

Personal Assurance Level
and
Electronic Assurance Level

State of Utah

Version as of September 5-, 2000
Current version may be found at:
www.cio.state.ut.us/399/digsigindex.htm

TABLE OF CONTENTS

Part 1 – Background

Part 2 – Policy Specification

PART 1 – BACKGROUND

Introduction

This document defines the Digital Signature Certificate Policy for use in the State of Utah. This document provides two ways in which entities and individuals may be authenticated. Entities and individuals may be authenticated through either personal presentment or through electronic processes. Each method contains its own Object Identifier (OID). **See** 1.2.

This policy reflects Utah's unique PKI environment. Utah licenses Certification Authorities (CAs) pursuant to Utah Code Annotated §§ 46 -3-101, et seq. and Utah Administrative Code §§ 154-10, et seq. This Policy restricts the use of certificates to those CAs who are licensed and in good standing with the State of Utah. As such, the requirements for a CA are not wholly found in this Policy, but are also found in the Utah Code and in the Utah Administrative Code.

This Policy employs technical concepts and acronyms associated with Public Key Infrastructure (PKI) technology. For those unfamiliar with this technology, a series of definitions, acronyms and explanations are provided in the introduction to the Policy . **See** 1.1.1 and 1.1.2.

Concepts

Certificate Policy

The X.509 standards define a Certificate Policy as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." Certificate Policies set forth the standards which digital signature certificates must comply with for common security and legal requirements. The CP establishes a level of trust that can be consulted by Subscribers and Relying Parties.

Certification Practice Statement

A Certification Practice Statement (CPS) is a "statement of the practices, which a Certification Authority employs in issuing certificates." Internet X.509 Public Key

Relationship between a Certificate Policy and a Certification Practice Statement

A CP sets forth the assurance that can be placed in a certificate. A CPS sets forth how a CA establishes that assurance. A CP may apply to more than just a single organization, but a CPS applies to only a single CA.

A Certificate Policy serves as the vehicle upon which to base common interoperability standards and common assurance criteria.

PART 2 – POLICY SPECIFICATION

1. Introduction

The Policy Specification portion of this document is modeled after and complies with the Internet Engineering Task Force Public Key Infrastructure X.509 (IETF PKIX) Part 4 Certificate Policy and Certification Practice Statement Framework.

1.1 Overview

The Certificate Policy defined in this document is intended for use by anyone who wants to conduct an electronic transaction with the State of Utah. Users of this document are to consult the issuing Certification Authority to obtain further details of the specific implementation of this Policy.

The digital signature policies within this Policy are for the management and use of Certificates used for verification, authentication, integrity and key agreement mechanisms. For instance, the Certificates issued under this Policy could be used for verifying the identity of electronic mail correspondents or for remote access to a computer system, verifying the identity of citizens or other legal entities, or protecting the integrity of software and documents.

Issuance of a certificate under this Policy does not imply that the Subscriber has any authority to conduct business transactions on behalf of an organization.

CAs are governed by the laws and rules of the State of Utah and any applicable federal and local law concerning the enforceability, construction, interpretation and validity of this Policy.

1.1.1 Policy Overview

This Policy defines the roles and responsiblities for CAs which issue certificates which reference this Policy and for Registration Authorities which must perform tasks that may be assigned to them by the CA. Subscribers and Relying Parties also have specific obligations which are outlined in this Policy.

A CA may issue cross-certificates at this level of assurance and is obliged to inform Subscribers which uses are intended within the State of Utah's PKI system.

A CA must ensure that it associates itself with, and uses, one Certificate and one CRL

A CA will revoke certificates in the circumstances enumerated in this Policy.

A CA is required to maintain records or information logs in the manner d escribed in this Policy.

A CA should ensure that critical CA functions are performed by at least two individuals.

~~Digital s~~Signature keys must not be backed-up or otherwise stored. Keys may have a validity period as indicated in this Policy.

This Policy does not allow for the recovery of private keys. The private key is in the sole possession of the Subscriber. Applications that require recoverable encrypted messaging will employ a CP defining confidentiality with key recovery for the encryption key ~~signature~~ only. Such applications may also use this CP, but only for a separate authentication key~~signature~~ and as long as there is no mingling of the two types of Certificates in a repository. Certificates based on this Policy rely on the Subscriber's sole possession to assert the right of Non-Repudiation and must not be mingled with any Certificates that allow recovery and thereby break the criteria of sole possession.

No personal information collected by a CA may be disclosed without the Subscriber's consent unless required by law. The CA may not sell any information under any circumstance that is not specifically allowed by this CP.

CA activities are subject to inspection by the Policy Authority (PA) and agents of the PA.

1.1.2 General Definitions

Approved CA- A Certification Authority which is licensed by the Division and approved by the PA.

Authenticate – The process which enables a party to confirm the identity or claims made by a party possessing a certificate.
Authority Revocation List (ARL) – A list of revoked CA certificates. An ARL is a CRL for CA cross-certificates.

CA – See "Certification Authority."

Certificate – The public key of a user, together with related information, digitally signed

Certificate Revocation List (CRL) – A list of certificates maintained by a Certification Authority of the certificates that it has issued and have since been revoked for any reason.

Certification Authority (CA) – An authority licensed by the Division to issue certificates.

Certification Practice Statement (CPS) – A statement of the practices, which a CA employs in issuing, suspending, revoking or otherwise managing its certificates.

Cross-Certificate – A certificate used to establish a trust relationship between two Certification Authorities.

Digital Signature – The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine:

(a) whether the transformation was created usi ng the key that corresponds to the signer's key; and
(b) whether the message has been altered since the transformation was made.

Distinguished Name (DN) – Data which unambiguously identifies the person or entity bearing the name.

Division – The Division of Corporations and Commercial Code within the Utah Department of Commerce.

Electronic Identification (EID) – An electronic process used to identify a subscriber. The process may employ measures which cross-references personal information against databases to ascertain the existence and reliability of that information.

End-Entity – An entity that uses the keys and certificates created within the PKI for purposes other than the management of the aforementioned keys and certificates. An End-Entity may be a Subscriber, a Relying Party, a device, or an application.

Entity – Any autonomous element within the Public Key Infrastructure. This may be a CA, an RA or an End-Entity.

Internet Engineering Task Force (IETF)- An open international community of

Licensed CA- A certification authority to whom a license has been issued by the Division and whose license is in effect.

Object Identifier (OID) – A specially formatted alphanumeric/numeric identifier that is registered with an internationally-recognized standards organization.

OID – See "Object Identifier."

Operative Personnel – Personnel acting as a Certification Authority or its agent, or in the employment of or under contract with a Certification Authority, and who have:

(a) managerial or policy making responsibilities for the certification authority; or

(b) duties directly involving the issuance of certificates, creation of private keys, or administration of a certification authority's computing facilities.

Personal Presentment – Refers to a method of subscriber identification whereby the subscriber attempts to establish his or her identity by personally presenting identification documents to a CA, RA, notary public or some other entity permitted by law or statute to perform registration authority duties.

Policy Authority (PA) – An entity designated by the Chief Information Officer for the State of Utah responsible for setting, implementing and administering policy decisions regarding CPs for the State of Utah.

Private Key – The key of a key pair used to create a digital signature. This key must be kept secret.

Public Key – The key of a key pair used to verify a digital signature. The public key is made widely available and is often published in a CA's repository.

Public Key Infrastructure – A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificate and keys.

RA – See "Registration Authority."

Registration Authority – An entity who authenticates certificate subjects, but does not sign or issue certificates.

Repository Service Provider (RSP) – An entity who performs repository services under the direction and control of an Approved CA.

1.1.3 Acronyms

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
EID	Electronic Identification
FIPS	(US) Federal Information Processing Standard
ITU	International Telecommunications Union
IETF	Internet Engineering Task Force
NIST	National Institute of Standards and Technology
OID	Object Identifier
PA	Policy Authority
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509

1.2 Identification Alphanumeric OID

Personal Assurance Level – OID to be assigned.

Electronic Assurance Level – OID to be assigned.

1.3 Community and Applicability

The State of Utah's PKI is managed by the Policy Authority as directed and designated by the Chief Information Officer for the State of Utah.

This Policy has been designed to enable the use of digital signatures as the equivalent of a handwritten signature. The State of Utah is not limited to this Policy and may issue, recognize or support additional Certificate Policies.

1.3.1 Certification Authorities

with their signature verification keys;
- promulgating certificate status through CRLs; and
- ensuring adherence to this Certificate Policy.

All Subscribers shall use CAs licensed by the Division and approved by the Policy Authority.

A CA may issue cross-certificates to other CAs licensed by the Division. A cross-certification must be in accordance with the selected Certificate Policy and any additional requirements as determined by the PA. A CA may issue cross-certificates to other CAs where expressly authorized by the PA.

1.3.2 Registration Authorities and Certificate Manufacturing Authorities

The role and functions of the Registration Authority (RA) shall be performed by each Approved CA. An Approved CA may subcontract Registration Authority functions to third party RAs who agree to be bound by this Policy, but the Approved CA remains responsible for the performance of those services in accordance with this Policy.

The role and functions of the Certificate Manufacturing Authority (CMA) shall be performed by each Approved CA. An Approved CA may subcontract CMA functions to third party CMAs who agree to be bound by this Policy, but the Approved CA remains responsible for the performance of those services in accordance with this Policy.

1.3.2.1 Repositories

The role and functions of the Repository shall be performed by each Approved CA. An Approved CA may subcontract performance of the Repository functions to a third party Repository who agrees to be bound by this Policy, provided that such subcontractor is approved in advance by the PA. The Approved CA remains responsible for the performance of repository services in accordance with this Policy.

1.3.2.2 Subscribers

A CA may issue Certificates that reference this Policy to the following classes of subscribers:

a) members of the general public ("Unaffiliated Individuals");
b) individuals associated with a sponsor recognized by the CA ("affiliated individuals"), provided the sponsor is the Subscriber of a valid Certificate

1.3.3 End Entities/Relying Parties

This Policy is intended for the benefit of the following persons who may rely on Certificates issued to others that reference this Policy.

- State of Utah government agencies.
- Federal or other government agencies that refer to this Policy.
- Businesses that agree to accept Certificates issued by a licensed CA and who agree to be bound by the terms of this Policy regarding those Certificates .
- Individuals that agree to accept Certificates issued by a licensed CA and who agree to be bound by the terms of this Pol icy regarding those Certificates.

1.3.4 Policy applicability

This Policy is suitable for the integrity and authentication of business transactions within the originator's approval limits and such that the falsification of the transaction would cause only minor financial loss or require only administrative action for correction.

1.3.5 Approved and Prohibited Applications

Certificates that reference this Policy are intended to support verification of digital signatures in applications where the identity of communicating parties needs to be:

1) authenticated;
2) where a message or file needs to be bound to the identity of its originator by a signature, and/or;
3) where the integrity of the file or message has to be assured.

Sample applications this Policy would be suitable for are:

- Personal or restricted information retrieval;
- Updating personal or restricted information;
- Filings with government agencies;
- Application processes, such as applying for government licenses, government benefits, etc.;
- Verifying the identity of communicating parties;
- Signing of electronic messages;
- Obtaining access to on-line data bases; and
- Classified/confidential communications between government agencies.

1.4 Contact Details

1.4.2 Contact Person

~~Robert Stewart~~ Al Sherwood
State Electronic Commerce ~~Digital Signature~~ Coordinator
State of Utah
Governor's Office, CIO Section
116 State Capitol
Salt Lake City, Utah 84114
Phone number: 801.538.1195~~862~~
Fax number: 801.538.1547
E-mail address: asherwoo@gov.state.ut.us ~~rstewart@gov.state.ut.us~~

1.4.3 Person Determining CPS Suitability for the Policy

~~No Stipulation.~~ Al Sherwood

2 General Provisions

2.1 Obligations

2.1.1 CA obligations

The CA is responsible for all aspects of the issuance and management of a certificate, including contro l over the application and enrollment process; the identification and authentication process; the actual certificate manufacturing process; publication of the certificate; suspension and revocation of the certificate; and renewal of the certificate; and for ensuring that all aspects of the CA Services and CA operations and infrastructure related to certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy.

The Approved CA is res ponsible and accountable for all actions performed by its employees, agents and subcontractors.

The CA will operate in accordance with its CPS, this Certificate Policy, and the Utah Code and Administrative Code when fulfilling these obligations. The CA wi ll take all reasonable measures to ensure that Subscribers and Relying Parties are aware of their respective rights and obligations with respect to the operation and management of any keys, Certificates or End-Entity hardware and software used.

2.1.1.1 Representations By CA

By issuing a certificate that references this Policy, the CA certifies to the Subscriber, and to all Relying Parties who reasonably and in good faith rely on the information contained in the certificate during its operational period and in acc ordance with this Policy, that:

(a) the CA has issued, and will manage, the certificate in accordance with this Policy;
(b) the CA has complied with the requirements of this Policy and its applicable CPS when authenticating the subscriber and issuing the certific ate;
(c) there are no misrepresentations of fact in the certificate known to the CA, and the CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS;
(d) information provided by the subscriber in the cer tificate application for inclusion in the certificate has been accurately transcribed to the certificate; and
(e) the certificate meets all material requirements of this Policy and the CA's CPS.

2.1.2 Registration Authority (RA) Obligations and Certification

The PA reserves the right to allow registration authority duties to be performed by governmental entities on behalf of their own employees. These arrangements must be approved by the PA and included in this Policy.

2.1.3 Subscriber Obligations

In all cases, the CA shall require the Subscriber to enter into an enforceable contractual commitment obligating the Subscriber to:

(a) take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;
(b) acknowledge that by accepting the Certificate the Subscriber is warranting that all information and representations made by the Subscriber that are included in the Certificate are true;
(c) use the Certificate exclusively for authorized and legal purposes, consistent with this Policy; and
(d) instruct the issuing CA to revoke the Certificate promptly upon any actual or suspected compromise of the Subscribers private key.

2.1.4 Relying Party Obligations

A Relying Party has a right to rely on a Certificate that references this Policy only if the Certificate was used and relied upon for lawful purposes and under circumstances where:

(a) the reliance was reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of reliance;
(b) the purpose for which the Certificate was used was appropriate under this Policy; and
(c) the Relying Party checked that the Certificate was valid prior to relying upon it.

2.1.5 Repository Obligations

The Approved CA is responsible for maintaining a secure system for storing and retrieving certificates. The Approved CA shall be responsible for providing a certificate and CRL repository for certificates that reference this policy. The CA may delegate performance of this obligation to an identified Repository Services Provider (RSP), provided that the CA remains primarily responsible for performance of those services by such third party in a manner consistent with the requirements of this Policy.

2.1.6 Policy Authority Obligations

The Policy Authority is responsible for the terms of this Policy and its administration.

2.2.2 RA and CMA Liability

An Approved CA shall be liable for all identification and authentication functions and all certificate manufacturing and issuing functions performed on its behalf by either an RA or a CMA.

2.2.3 Disclaimers of Warranties and Obligations

The State of Utah assumes no liability whatsoever in relation to the use of certificates or associated public/private key pairs for any use.

The State of Utah, its employees and agents makes no representations, warranties or conditions, express or implied other than as expressly stated in this CP or in any other official document.

2.3 Financial Responsibility

2.3.1 CA Financial Responsibility

An issuing CA shall meet the greater of the responsibilities outlined here or those established in another CP the issuing CA is approved for, that is, the CA is to meet the greater *set* of responsibilities not the *sum* of the responsibilities.

All Approved CAs must comply with the statutory and regulatory requirements as administered by the Division. As such, CAs must comply with specific financial obligations in order for the CA to continue in good standing. A CA whos e license is in good standing is deemed to have satisfied the financial obligations under this CP. However, the PA retains the ability to add any financial/insurance requirements with 30 days notice, in addition to the licensing requirements the Division may require.

2.3.2 Consequences of Failure to Meet Financial Responsibilities

The failure of a CA to continuously maintain either its insurance or bond coverage may be the basis for revocation or suspension of its approval to issue certificates under this CP and may also be the basis for revocation or suspension of its approval to conduct activities for certificates previously issued.

2.4.2 Severability, Survival, Merger, Notice

Any CA, or agent of a CA, shall ensure that any of its agreements will have appropriate provisions governing severab ility, survival, merger or notice.

2.4.3 Dispute Resolution Procedures

Each CA shall ensure that any agreement it enters into provides appropriate dispute resolution procedures.

2.5 Fees

A CA may not impose any fees on the reading of this Policy or its CPS.

Subscriber fees are subject to agreement between the CA and the Subscriber and must be in accordance with a fee schedule published by the CA in its CPS or in another publicly available medium.

2.6 Publication and Repository

2.6.1 Publication of CA Information

Each Approved CA shall operate a secure on -line Repository that is available to Relying Parties and contains:

(1) Certificates that reference this Policy;
(2) a Certificate Revocation List ("CRL") or on -line certificate status database;
(3) the CA's Certificate for its signing key;
(4) past and current versions of the CA's CPS;
(5) a copy of (or a link to) this Policy; and
(6) other relevant information relating to Certificates that reference this Policy.

2.6.2 Frequency of Publication

All information to be published in t he Repository shall be published promptly after such information is available to the CA. Certificates issued by the CA that reference this Policy will be published promptly upon acceptance of such Certificate by the Subscriber.

2.7 Compliance Audit

All Approved CAs must comply with the statutory and regulatory requirements as administered by the Division. As such, CAs mus t comply with specific audit requirements in order for a CA to continue in good standing. A CA whose license is in good standing is deemed to have satisfied the audit requirements under this CP. However, the PA retains the ability to add any audit requir ements with 30 days notice, in addition to the licensing requirements the Division may require. **See** U.C.A. § 46-3-202; Utah Admin. Code R154 -10-106, 402 and 403.

2.8 Confidentiality Policy

Information regarding Subscribers that is submitted on application s for Certificates will be kept confidential by the CA and shall not be released without the prior consent of the Subscriber, unless otherwise required by law. This does not apply, however, to information appearing on certificates.

2.8.1 Types of Information to be Kept Confidential

Each CA shall protect the confidentiality of personal information regarding Subscribers that is collected during the entire certificate life cycle process.

Under no circumstances shall a CA have access to the private keys of any subscriber to whom it has issued a certificate.

2.8.2 Types of Information not Considered Confidential

Information appearing on certificates, which the Subscriber has consented to publish, is not considered confidential.

2.9 Intellectual Property Rights

No stipulation.

3 Identification and Authentication

3.1 Initial Registration

Certificate applications may be communicated from the applicant to the CA or an RA, and authorizations to issue certificates may be communicated from an RA to the CA. The communications may be submitted:

1) electronically, provided the communications are secure, by using SSL or a similar security protocol;
2) by first class U.S. mail; or
3) in person.

3.1.1 Types of Names

The subject name used for applicants in the certificate shall be a unique X.50~~09~~ Distinguished Name (DN).

3.1.2 Need for Names to be Meaningful

The subject name listed in a Certificate must have a reasonable association with the authenticated name of the Subscriber. In the case of individuals this should be a combination of first name and/or initials and surname. In the case of an organization the name should reflect the legal name of the organization and/or unit.

A Certificate that refers to a role or position shall also contain the identity of the person who holds that role or position.

Any Certificate issued for a device or application shall, within the DN, include the name of the person or organization responsible for that device or application.

3.1.3 Rules for Interpreting Various Name Forms

No stipulation.

3.1.4 Uniqueness of Names

The subject name listed in a Certificate shall be unique for all certificates issued by the CA. If necessary, additional numbers or letters may be appended to the real name to ensure the DN's uniqueness within the domain of certificates is sued by the CA.

3.1.7 Method to Prove Possession of Private Key

The CA shall establish that the applicant is in possession of the private key corresponding to the public key submitted with the application in accordance with an appropriate secure protocol, such as that described in the IETF PKIX Certificate Management Protocol.

3.1.8 Authentication of Organization Identity

An application for an organization to be a Subscriber may be made by an individual or an organization authorized to act on behalf of the prospective Subscriber.

The CA or RA must verify the identity and authority of the individual or organization acting on behalf of the prospective Subscriber and their authority to receive the keys on behalf of that organization.

The CA must examine documentation providing evidence of the existence of the organization at the business address listed in the certificate application.

In conducting its review and investigation, the CA shall review official government records and/or engage the services of a reputable third party vendor of business information to provide validation information concerning each organization applying for a certificate, including legal company name, type of entity, year of formation, names of directors and officers, address, telephone number, and good standing in the jurisdiction where the applicant is incorporated or otherwise organized.

The CA will keep records of the type and details of identification used.

3.1.9 Authentication of Individual Identity

There are various authentication practices employed in PKI systems. Authentication measures may vary according to market practices and legal requirements. This Policy seeks to give flexibility to meet demands for different applications in a changing and dynamic electronic commerce environment.

The Personal Assurance level of authentication is the default standard for the State of Utah. Applications that do not specify what level of authentication is desired will automatically fall under the purview of the Personal Assurance requirements.

Any entity seeking to use the Electronic Assurance authentication requirements must first get approval from the PA.

-The CA must have evidence of at least one of the following:

1) a birth certificate issued in the United States;
2) a driver's license issued by a State of the United States;
3) a personal identification card issued by a State of the United States;
4) a United States passport; or
5) other evidence if the PA has given written approval prior to the issuance of the certificate.

Electronic Assurance Authentication Requirements

-The licensed CA confirms the identification of a subscriber through protocols that include Electronic Identification (EID) processes. EID may only be used to the extent that the PA has approved the particular process and/or company.

3.1.10 Authentication of Devices or Applications

An application for a device or application to be an End -Entity may be made by a Subscriber for whom the device's or application's signature is attributable for the purposes of accountability and responsibility.

Identification and authentication of the applicant must follow this Policy's requirements as if the Subscriber was applying for the Certificate on its own behalf.

The device Certificate will be revoked if the Subscriber's Certificate is revoked.

3.2 Renewal Applications (Routine Rekey)

A request for rekey may only be made by the entity in whose name the keys have been issued. All requests for rekey must be authenticated by the CA, and the subsequent response must be authenticated by the entity in whose n ame the keys have been issued. If one of the keys has expired the request for rekey must be authenticated in the same manner as the initial registration.

3.3 Rekey After Revocation

A revoked, expired or compromised Certificate may not be renewed. Any sub sequent request for renewal or rekey must occur in the same manner as the initial registration.

3.4 Revocation Request

A CA or RA must authenticate a request for revocation of a certificate. A CA must

4 Operational Requirements

4.1 Certificate Application

A CA must ensure that its procedures and requirements with respect to an application for a certificate are set out in its CPS.

A CA must ensure that each application be accompanied by:

1) proof of the Subscriber's identity;
2) proof of authorization for any requested certificate attributes;
3) a signed agreement, of the applicable terms and conditions governing the use of a certificate; and
4) a public verification key generated by the Subscriber.

Certificate applications may be initiated by the Subscriber, or a party who has written authorization to be a representative of the sponsor or the subscribing organization.

4.1.1 Application for a Cross-Certificate

The PA will identify the necessary procedures to apply for a cross-certificate.

An application for a cross-certificate does not oblige the PA to authorize a cross-certificate. The PA shall review any CA's request for cross-certification and approve or deny any such request.

A CA requesting cross-certification will include with the application:

- its Certificate Policy;
- an external audit inspection report validating the assurance level stated in the CP;
- the public verification key generated by the CA .

4.2 Certificate Issuance

Upon successful performance of all required application processes including identification and authentication of the subscriber, the CA may issue and publish the certificate indicating complete and final approval of the certificate application.

4.3 Certificate Acceptance

A CA must ensure that a Subscriber acknowledges acceptance of a certificate. The CA

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

A certificate must be revoked:

- when any information in the certificate changes;
- upon suspected or known compromise of the private key;
- upon suspected or known compromise of the media holding the key; or
- upon the request of the Subscriber or sponsoring organization.

A CA, in its discretion, may revoke a certificate when an entity fails to comply with obligations set out in this CP, any agreement or any applicable law.

The PA, in its discretion, may revoke a cross-certificate when a CA fails to comply with obligations set out in this CP ~~, any agreement~~ or any applicable law.

4.4.2 Who Can Request Revocation

The revocation of a certificate may only be requested by:

- the Subscriber in who name the certificate was issued;
- the individual or organization which made the application for the certificate on behalf of a device or application;
- the Sponsor;
- the personnel of the Issuing CA; or
- personnel of an RA working with the Issuing CA.

The revocation of a cross-certificate may only be requested by:

- the CA on whose behalf the cross-certificate was issued; or
- the PA.

4.4.3 Procedure for Revocation Request

A CA must ensure that its procedures and requirements with respect to the revocation of a certificate are set out in the CPS or otherwise made publicly available. An authenticated revocation request, and any resulting actions taken by the CA, must be recorded and retained. In the case where a certificate is revoked, justification for the revocation must also be documented.

Where an Entity certificate is revoked, the revocation will be published in the appropriate CRL. Where a cross-certificate is revoked, the revocation will be published in the ARL of

4.4.5 Circumstances for Suspension
Certificate suspension is not permitted under this Policy.

4.4.6 Who Can Request Suspension
No stipulation.

4.4.7 Procedure for Suspension Request
No stipulation.

4.4.8 Limits on Suspension Period
No stipulation.

4.4.9 CRL Issuance Frequency
A CA must ensure that it issues an up -to-date CRL at least every twenty-four hours.

When a certificate is revoked due to key compromise the updated CRL must be issued immediately.

A CA must also ensure that its CRL issuance is synchronized with any d irectory synchronization to ensure the accessibility of the most recent CRL.

4.4.10 CRL Checking Requirements
A Relying Party must check the status of all certificates in the certificate validation chain against the current CRLs and ARLs prior to their use. A Relying Party must also verify the authenticity and integrity of CRLs and ARLs.

4.4.11 On-Line Revocation/Status Checking Availability
On-line certificate revocation/status checking is optional under this Policy.

4.4.12 On-Line Revocation checking Requirements
No stipulation.

4.4.13 Other Forms of Revocation Advertisements Available
No stipulation

4.4.15 Special Requirements Regarding~~key~~ Compromise

In the event of the compromise or suspected compromise, of a CA signing key, a CA must immediately notify all CAs to whom it has issued cross-certificates and the PA.

In the event of the compromise or suspected compromise, of any other Entity's signing key, the Entity must immediately notify the issuing CA.

A CA must ensure that provisions outlining the means it will use to provide notice of compromise or suspected compromise are in its CPS or a publicly-available document and appropriate agreements.

4.5 Security Audit Procedures

All Approved CAs must comply with the statutory and regulatory requirements as administered by the Division. As such, CAs must comply with specific audit requirements to continue in good standing. A CA whose license is in good standing is deemed to have satisfied the audit requirements under this CP. However, the PA retains the ability to add any audit requirements with 30 days notice, in addition to the licensing requirements the Division may require. **See** U.C.A. § 46-3-202; Utah Admin. Code R154-10-106, 402 and 403.

4.5.1 Types of Events Recorded

A CA should record in audit log files all events relating to the security of the CA system. These include such events as:

- system start-up and shutdown;
- CA application start-up and shutdown;
- attempts to create, remove, set passwords or change the system privileges of operative personnel;
- changes to CA details and/or keys;
- changes to certificate creation policies;
- login and logoff attempts;
- unauthorized attempts at network access to the CA system;
- unauthorized attempts to access system files
- generation of own and subordinate Entity keys;
- creation and revocation of certificates;
- attempts to initialize remove, enable, and disable Subscribers, and update and

- physical access logs;
- system configuration changes and maintenance;
- personnel changes;
- discrepancy and compromise reports;
- records of the destruction of media containing key material, activation data, or personal Subscriber information.

A CA must ensure that the CPS indicates what information is logged.

To facilitate decision-making, all agreements and correspondence relating to CA services should be collected and consolidated, either electronically or manually, in a single location.

4.5.2 Frequency of Processing Log

A CA must ensure that its audit logs are reviewed by CA personnel at least once every week and all significant events are explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken as a result of these reviews must be documented.

4.5.3 Retention Period for Audit Log

A CA must retain its audit logs on-site for at least two months.

4.5.4 Protection of Audit Log

Manual or electronic audit logs must be protected from unauthorized viewing, modification, or deletion.

4.5.5 Audit Log Backup Procedures

Audit logs and audit summaries must be backed up or copied if in manual form. The back up procedures must occur at least monthly.

4.5.6 Audit Collection System (Internal v. External)

A CA must identify its audit collection systems in its CPS.

4.5.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system no notice need be given to the individual, organization, device or application which caused the event.

4.6 Records Archival

4.6.1 Types of Records Archived

The following data and files must be archived by or on behalf of the CA:

- all audit data as detailed in 4.5;
- all certificate application data including subsc riber agreements, and identification and authentication data;
- certificate and revocation requests;
- all certificates issued or published;
- CRLs, ARLs issued or certificate status records generated;
- documentation required by compliance auditors;
- key histories; and
- all correspondence between the CA and RAs, CMAs, RSPs, and/or subscribers.

The CA is responsible for the satisfactory archiving of this material.

4.6.2 Retention Period for Archive

Certificates and private keys must be archived for at least 1 year after the expiration of the key material.

Audit information as detailed in 4.5, subscriber agreements and any identification and authentication information should be retained for at least 7 years.

In the absence of a specific retention period any record or item shall be retained for a period of no less than 7 years.

Any signed document may also have public records retention requirements that must also be met.

4.6.3 Protection of Archive

The archive media must be protected either by physical security alone, o r a combination of physical and cryptographic protection. Archive sites must provide adequate protection from environmental threats such as temperature, humidity and magnetism.

4.6.4 Archive Backup Procedures

4.6.6 Archive Collection System (Internal Or External)

A CA must identify its archiv e collection systems in its CPS.

4.6.7 Procedures to Obtain and Verify Archive Information

During the compliance audit required by this Policy, the auditor shall verify the integrity of the archives.

4.7 Key Changover

A CA must identify the details of its ke y changeover procedures in its CPS. Subscribers without valid keys must be re -authenticated by the CA or RA in the same manner as the initial registration. Keys may not be renewed using an expired Digital Signature key.

4.8 Compromise and Disaster Recovery

4.8.1 Computing Resources, Software, and/or Data are Corrupted

A CA must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data. Where a repository is not under the control of the CA, a CA must ensure any agreement with the repository provides that business continuity procedures be established and documented by the repository. The business continuity procedures must be referenced within a CA's CPS.

4.8.2 Entity Public Key is Revoked

In the event of the need for revocation or downgrade of a CA's public key, the CA must immediately notify the PA; the CAs to whom it has issued cross -certificates; its RAs; all subscribers; and all individuals or organiza tions who are responsible for a certificate used by a device or application.

In the case of revocation, the CA must also publish the public key serial number on an appropriate CRL; revoke all cross -certificates signed with the revoked public key. After the factors that led to revocation, the CA may generate a new CA signing key pair and re - issue certificates to all Entities and ensure all CRLs and ARLs are signed using the key.

4.8.3 Entity Key is Compromised

4.8.4 Secure Facility after a Natural or Other Type of Disaster

A CA must establish a disaster recovery plan outlining the steps to be taken to re - establish a secure facility in the event of a natural disaster. Where a reposito ry is not under the control of the CA, a CA must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

4.9 CA Termination

In the event that a CA ceases operation, it must notify its Subscribers; sponsoring organizations; Ras; CMAs; RSPs; CA's with whom it is cross -certified; and Relying Parties. After the CA ceases operation it must arrange for the continued retention of the CA's keys and information. All certificates issued by the CA that reference this Policy will be revoked no later than the time of termination. All current and archived CA identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data shall be transf erred to the PA (or designate) within 72 hours of CA cessation.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Controls

5.1.1 & 5.1.2 Site Location, Construction and Physical Access

The CA site must be consistent with facilities used to house high -value sensitive information. The CA must:

- implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing CA Services;
- restrict physical access to the CA site and use manual or electronic protection mechanisms for unauthorized intrusion at all times;
- The CA maintain a current site access log and ensure personnel not on the access list are properly escorted and supervised.

The CA is responsible to ensure that affiliated RAs implement appropriate physical security to the hardware and information in their control.

5.1.3 Power and Air Conditioning

A CA must ensure that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water Exposures

A CA must ensure that the CA system is protected from water exposure.

5.1.5 Fire Prevention and Protection

A CA must ensure that the CA system is protected with a fire suppression system.

5.1.6 Media Storage

A CA must ensure that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

5.1.7 Waste Disposal

A CA must ensure that media used to store or transmit sensitive information such as keys,

5.2 Procedural Controls

5.2.1 Trusted Roles

5.2.1.1 CA Trusted Role

A CA must ensure a separation of duties for critical CA functions to prevent one person from maliciously using the CA system and the root key without detection.

A CA must distinguish between day-to-day operations of the CA system from the management and audit of those operations.

A CA must explain the separation of trusted roles in its CPS.

5.2.1.2 RA Trusted Role

The primary responsibilities of the RA include acceptance of certificate applications; certificate changes; certificate revocations; key recovery requests; verification of an applicant's identity and authorizations; transmissions of an applicant's information to the CA; and provision of authorization codes for on-line key exchange and certificate creation.

A CA must explain the role of its RA's in its CPS.

5.2.2 Number of Persons Required Per Task

To ensure that one person acting alone cannot circumvent safeguards, responsibilities at a CA server must be distributed among different individuals. Each account on the CA server shall have limited capabilities commensurate with the role of the account holder.

5.2.3 Identification and Authentication for each Role

All CA personnel must have the identity and authorization verified before they are included in the access list for the CA site, given access to the CA system and given an account on the PKI system. CA operations must be secured using mechanisms such as token-based strong authentication and encryption, when accessed across a shared network.

5.3 Personnel Controls

A CA must ensure that all personnel performing duties with respect to the operation of a

5.3.1 Background, Qualifications, Experience and Clearance Requirements

A CA and its affiliated RAs, CMAs and RSPs must have personnel policies sufficient to provide reasonable assurance that its personnel have the background, qualifications and experience to perform their duties with respect to the operation of a trustworthy system.

5.3.2 Background Check Procedures

CAs are required to perform a criminal background check of operative personnel. **See** Utah Admin. Code R154 -10-107. All personnel who fail an initial or periodic background check may not serve or continue to serve in a trusted role.

5.3.3 Training Requirements

A CA must ensure that all personnel performing duties with respect to the operation of a CA or RA, receive comprehensive training in:

- the CA/RA security principles and mechanisms;
- all PKI software versions in use on the CA system;
- all PKI duties they are expected to perform; and
- disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

Training requirements must be kept current and given as often as required to ensure personnel are performing their duties appropriately.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

No stipulation.

5.3.7 Contracting Personnel Requirements

No stipulation.

5.3.8 Documentation Supplied to Personnel

A CA must ensure that its personnel and affiliated RAs, CMAs and RSPs have access to the certificate policies it supports, its CPS, and any relevant statutes, policies or contracts.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Each prospective certificate holder must generate its own Digital Signature key pair using a PA-approved algorithm.

6.1.2 Private Key Delivery to Entity

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

The public verification key m ust be delivered to the CA via an on -line transaction in accordance with the PKIX -3 Certificate Management Protocol, or via an equally secure manner.

6.1.4 CA Public Key Delivery to Users

The CA public verification key must be delivered to the prospective certificate holder via an on-line transaction in accordance with the PKIX -3 Certificate Management Protocol, or via an equally secure manner.

6.1.5 Key Sizes

A CA must ensure that key pairs for all PKI entities use at least 1024 bit RSA or DSA or 2048 bit RSA.

6.1.6 Public Key Parameters Generation

A CA that utilizes DSA must generate parameters in accordance with FIPS 186.

6.1.7 Parameter Quality Checking

Not applicable.

6.1.8 Hardware/Software Key Generation

6.2 Private Key Protection

The CA (and the RA, CMA, and RSP) shall each protect its private ke y(s) in accordance with the provisions of this Policy.

The certificate holder assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure. **See** U.C.A. § 46-3-305.

6.2.1 Standards for Cryptographic Module

Refer to 6.8.

6.2.2 Private Key (N-M) Multi-Person Control

Private signing keys require at least two people for CA key generation operations.

6.2.3 Private Key Escrow

Digital Signature private keys may not be escrowed. Encryption keys may be escrowed.

6.2.4 Private Key Backup

An entity may optionally back up its own private key. Encryption keys may be backed up.

6.2.5 Private Key Archival

An entity may optionally archive its own private key. Encryption keys may be archived.

6.2.6 Private Key Entry into Cryptographic Module

No stipulation.

6.2.7 Method of Activating Private Key

Entities must be authenticated prior to the activation of the private key. This authentication may be in the form of pass -phrases or PINs in a cryptomodule.

6.2.8 Method of Deactivating Private Key

When keys are deactivated they must be cleared from memory before the memory is de -allocated. Any disk space where keys were stored must be over -written before the space

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival
The issuing CA must retain all verification public keys.

6.3.2 Usage Periods for the Public and Private Keys
All keys must have validity periods of no more than six years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation
Activation data must have an appropriate level of strength for the keys or data to be protected. Activation data must be unique and unpredictable. If activation data is transmitted it must done in an appropriately protected manner.

6.4.2 Activation Data Protection
Data used to unlock private keys for initialization must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms.

6.4.3 Other Aspects of Activation Data
No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements
Each CA server must include the following functionality:

- access control to CA services and PKI roles;
- enforced separation of duties for PKI roles;
- identification and authentication of PKI roles and associated identities;
- object re-use or separation for CA random access memory;
- use of cryptography for session communication and database security;
- archival of CA and End -Entity history and audit data;
- audit of security related events;

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The CA must use software that has been designed and developed under a formal development methodology. The CA software must have third party verification.

6.6.2 Security Management Controls

The configuration of the CA system as well as any modifications and upgrades must be documented and controlled. The CA must ensure there is a method of detecting unauthorized modifications to the CA software or configuration.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

The CA server must be protected from attack through any open or general purpose network with which it is connected. The protection must be provided through the installation of a device configured to allow only the protocols and commands required for the operation of the CA. A CA must ensure that its CPS defines these protocols and commands.

6.8 Cryptographic Module Engineering Controls

All CA cryptographic operations must be performed in a cryptographic module validated to at least FIPS 140-1 Level 1 or to an equivalent level of functionality and assurance. RA operations must be validated to at least FIPS 140-1 Level 1 or to an equivalent level of functionality and assurance.

End Entities must use cryptographic modules validated to FIPS 140-1 level 1 or to an equivalent level of functionality and assurance.

7 Certificate and CRL Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

All certificates that reference this Policy will be issued in the X.509 version 3 format and will include a reference to the OID for this Policy within the appropriate field.

PKI End-Entity software must support the following X.509 fields:

- Signature - CA signature to authenticate a certificate;
- Issuer – name of issuing CA;
- Validity – activation and expiration date for certificate;
- Subject – subscriber's distinguished name;
- Subject Public Key Information – algorithm ID, key;
- Version – version of X.509 certificate
- Serial Number – unique serial number for certificate.

7.1.2 Certificate Extensions

The CPS must identify the certificate extensions supported by the CA, its RA and End Entities.

~~The "certificatePolicies" field must be set as critical in all certificates that reference this policy.~~

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP must use the following OIDs for signatures:

- RSA 1024 – OID TBD
- SHA-1 –OID TBD

7.1.4 Name Forms

Every DN must be in the form of an X.501 "printableString."

7.1.7 Usage of Policy Constraints Extension

A CA must populate and mark as critical the “policyConstraints” extension.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy

Critical extensions must be interpreted as defined in PKIX.

7.2 CRL Profile

7.2.1 Version Number

A CA must issue X.509 version 2 CRLs in accordance with the PKIX Certificate and CRL Profile.

7.2.2 CRL and CRL Entry Extensions

All Entity PKI software must correctly process all CRL extensions identified in the Certificate and CRL profile. The CPS must define the use of any extensions support ed by the CA, its RAs and End Entities.

8 Specification Administration

8.1 Specific Change Procedures

8.1.1 Notification of Changes

The PA will notify all approved CAs before any changes are made to this Policy.

8.1.2 List of Items

All items in this Policy are subject to the notification requirement.

8.1.3 Notification Mechanisms

The PA will notify via email, preferably secure, all approved CAs of any proposed changes to this Policy. The notification must contain a statement of pr oposed changes, the final date for receipt of comments, and the proposed effective date of the change. The PA may request CAs to notify their Subscribers of the proposed changes.

8.1.4 Mechanism to Handle Comments

Written and signed comments on propose d changes must be directed to the PA. Decisions with respect to the proposed changes are at the sole discretion of the PA.

8.1.5 Comment Period

The comment period will be 30 days unless otherwise specified. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change must be given with a final change notice.

8.2 Publication and Notification Policies

A copy of this Policy is available in electronic form at ~~http:www.~~ **www.cio.state.ut.us/399/digsigindex.htm**

Approved CAs shall post copies of this Policy (or links thereto) in their repositories.